Special Alerts

SA-185-2009
October 29, 2009

TO:	CHIEF EXECUTIVE OFFICER (also of interest to BSA Compliance and Security Officer)
SUBJECT:	Fraudulent Work-at-Home Funds Transfer Agent Schemes
Summary:	*Individuals are using deposit accounts to receive unauthorized electronic funds transfers and forward funds overseas to criminals.*

The Federal Deposit Insurance Corporation (FDIC) is warning financial institutions of an increase in schemes to recruit individuals to receive and transmit unauthorized electronic funds transfers (EFTs) from deposit accounts to individuals overseas. These funds transfer agents, often referred to as "money mules," are typically solicited on the Internet by criminals who have gained unauthorized access to the online deposit account of a business or consumer. In a typical scenario, the criminal will originate unauthorized EFTs from a victim's account to a money mule's deposit account. The money mule is then instructed to quickly withdraw the funds and wire them overseas after deducting a "commission" (commonly eight to ten percent).

Criminals target online deposit accounts at institutions where business customers can originate EFTs, such as automated clearing house (ACH) and wire transfers, over the Internet. Money mules, however, can be customers at any depository institution where EFTs can be received and funds withdrawn. In some cases, the money mule may be an unknowing accomplice in a fraud scheme. Because EFTs are often made immediately available by the receiving institution, funds may be removed and wire transferred overseas before the fraud is detected. Refer to SA-147-2009 http://www.fdic.gov/news/news/specialalert/2009/sa09147.html for more information on fraudulent EFT schemes.

Money mule schemes can take many different forms, but most involve receiving unauthorized EFTs into a deposit account and then withdrawing the funds or forwarding them on to another party via another EFT. The following are common scenarios:

- Online job posting Web sites are used by criminals to locate individuals seeking employment with flexible work hours that can be performed from home. These work-at-home schemes often involve written employment contracts, job descriptions and procedures to legitimize the scam.
- Advance fee scams promising large monetary rewards for acting as a financial intermediary can entice individuals to participate in this activity.
- Mystery shopping jobs may be used that require the employee to assess the performance of money service businesses by completing EFTs and then evaluating the service using customer satisfaction forms.
- Social networking sites may be used to recruit individuals to act as money mules. Criminals conjure up various imaginative stories to befriend and persuade individuals to receive and forward stolen funds.
- Some hesitant or skeptical money mules have been intimidated, harassed and threatened by their criminal "employers" to process the funds transfers quickly and with secrecy.
- The personal identifiable information provided by the money mule might later be used to commit identity theft or account takeover.

The following are examples of events that may indicate money mule account activity:

- A deposit account opened with a minimal deposit soon followed by large EFT deposits.
- Deposit customers who suddenly begin receiving and sending EFTs related to new employment, investments, business opportunities or acquaintances (especially opportunities found on the Internet).

- A newly opened deposit account with an unusual amount of activity, such as account inquiries, or a large dollar amount or high number of incoming EFTs.
- An account that receives incoming EFTs then shortly afterward originates outgoing wire transfers or cash withdrawals approximately eight to ten percent less than the incoming EFTs.
- A foreign exchange student with a J-1 Visa and fraudulent passport opening a student account with a high volume of incoming/outgoing EFT activity.

Money mule activity is essentially electronic money laundering addressed by the Bank Secrecy Act and Anti-Money Laundering Regulations. Strong customer identification, customer due diligence, and high-risk account monitoring procedures are essential for detecting suspicious activity, including money mule accounts. Financial institutions can find additional guidance about customer identification, account monitoring, suspicious activity reporting, and identity theft red flags below:

FDIC Risk Management Manual of Examination Policies - Bank Secrecy Act
www.ffiec.gov/bsa_aml_infobase/documents/FDIC_DOCs/BSA_Manual.pdf;

FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual
www.ffiec.gov/bsa_aml_infobase/default.htm and

FFIEC Identity Theft Red Flags – Interagency Final Regulations and Guidelines
www.fdic.gov/news/news/financial/2007/fil07100.pdf

Financial institutions should act promptly when they believe fraudulent or improper activities have occurred, such as those of a money mule. Appropriate actions may include, but are not limited to, filing a Suspicious Activity Report and/or closing the deposit account in accordance with existing, board-approved account closure policies and procedures.

Cyber-fraud incidents and other fraudulent activity may be forwarded to the FDIC's Cyber-Fraud and Financial Crimes Section, 550 17th Street, N.W., Room F-4004, Washington, D.C. 20429, or transmitted electronically to alert@fdic.gov. Questions related to federal deposit insurance or consumer issues should be submitted to the FDIC using an online form that can be accessed at http://www2.fdic.gov/starsmail/index.asp.

For your reference, FDIC Special Alerts may be accessed from the FDIC's website at http://www.fdic.gov/news/news/specialalert/2009/index.html. To automatically receive FDIC Special Alerts through e-mail, please visit www.fdic.gov/about/subscriptions/index.html.

Sandra L. Thompson
Director
Division of Supervision and Consumer Protection

Distribution: FDIC-Supervised Banks (Commercial and Savings)

Note: Paper copies of FDIC Special Alerts may be obtained through the FDIC's Public Information Center, 1-877-275-3342 or 703-562-2200.

Last Updated 10/29/2009 communications@fdic.gov